DEPARTMENT OF THE ARMY
HEADQUARTERS, 4th INFANTRY DIVISION (MECHANIZED)
FORT HOOD, TEXAS 76544-5200

REPLY TO
ATTENTION OF

AFYB-CG 4 AUGUST 2004

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Information Systems and Network Security

1. REFERENCES.

a. Fort Hood Command Policy Number DOIM-01, Computer Network Security, 2 April 04.

b. AR 21-1, Army Information Management, 30 June 2004.

c. AR 25-2, Information Assurance, 14 November 2003.

2. This policy applies to all 4ID personnel and units that utilize Information Systems on the Fort Hood SIPR and NIPR Networks (SIPRNet and NIPRNet).

3. In order to assure security of the Fort Hood Network and operational information, commanders and leaders at all levels will ensure compliance with the following:

a. All Installation Local Area Network (ILAN, also called NIPRNet) users must log into the Hood domain when connected to the installation infrastructure.

b. All network devices connected to the network or stand-alone, will comply with the Department of the Army published Information Assurance Vulnerability Management (IAVM) directives, network security procedures, and the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP).

c. Users of both ILAN and SIPRNet are responsible for the proper use of equipment. Under no circumstances will a subscriber move, alter, place an attachment on, or make any additions to network information systems, to include, but not limited to, hubs, routers, switches, and any multi-port devices.

d. Users will take all precautions to ensure that no device capable of storing information is transferred from the SIPRNet to the NIPRNet. Exceptions must be approved and supervised by the G6 and G2.

e. Users establishing shared folders and other network resources will password protect these resources with passwords in compliance with Fort Hood standards. The establishing user is responsible for limiting access to these resources to the appropriate personnel.

f. No operational or tactical information will be written, placed, or otherwise established on the NIPRNet. This information will only be used only on the SIPRNet.

g. Failure to follow any of the above procedures and proper security policies and regulations for accessing an Internet/Intranet website(s) will result in immediate suspension of network access and privileges until compliance is confirmed.

h. All units and headquarters sections will appoint an Information Management Officer (IMO),an Information Assurance Security Officer (IASO), and a Systems Administrator (SA). IASOs will be trained and certified through Level I and SAs will be certified through Level II of the System Administration Security/Network Management Security program.

i. All Brigade and Separate Unit S6s and/or IMOs will inventory 100% of their units' information systems and report to the G6. Monthly updates will be submitted by the 1st of each month.

j. The G6 will:

(1) Establish standardized patch and virus scanning management policies, procedures, and tools.

(2) Coordinate with the Directorate of Information Management (DOIM) for network monitoring information concerning all network vulnerabilities.

(3) Monitor division-wide compliance with Information Systems directives and policies.

(4) Coordinate with the DOIM for Level I and II training for IASOs and SAs.

(5) Conduct risk assessments and report findings as required by regulation.

4. POC for the policy is the Division G-6 at 618-8023.

//original signed//
JAMES D. THURMAN
Major General, USA
Commanding